UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/574,010	03/29/2006	Yoshihide Nakane	127546	4333

25944 7590 09/28/2010

OLIFF & BERRIDGE, PLC
P.O. BOX 320850
ALEXANDRIA, VA 22320-4850

EXAMINER	
KING, CURTIS J	

ART UNIT	PAPER NUMBER
2612	

NOTIFICATION DATE	DELIVERY MODE
09/28/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

OfficeAction25944@oliff.com
jarmstrong@oliff.com

Office Action Summary	Application No.	Applicant(s)	
	10/574,010	NAKANE, YOSHIHIDE	
	Examiner	Art Unit	
	Curtis J. King	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 & 6-12* is/are rejected.

7)☒ Claim(s) *5* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Onuma (Pub. No.: US 2001/0026213 A1) in view of von Alten (Pat. No.: US 6,873,840 B1), Nakarmura (EP 1 286 297 A1), and Asakura (Pat. No.: US 6,744,349 B1).

1) In regard to claim 1, Onuma discloses the claimed anti-theft system for a vehicle (fig. 1: 1), comprising:

a certifying device of an electronic key for getting in the vehicle (fig. 1: 11 discloses as a passive control unit), the certifying device certifying the electronic key held by a person who intends to get in the vehicle (¶0036);

a door lock control device (fig. 1: 13 discloses as an unlock and lock controller) that unlocks a vehicle door in a case where the electronic key is certified by the certifying device of the electronic key for getting in the vehicle in a state where the door is locked (¶0036);

a memory (fig. 1: 11b) that memorizes ID information of the electronic key when the vehicle door is unlocked by the door lock control device based on the electronic key

being certified by the certifying device of the electronic key for getting in the vehicle (¶0050);

a certifying device of an electronic key for starting an engine (fig. 1: 11 discloses as a passive control unit), the certifying device certifying the electronic key based on whether ignition knob is operated by a driver (¶0052) and reception of a response signal sent from the electronic key held by a person who intends to start the engine (¶0056); and

an engine starting switch (fig. 3: 30 discloses as an ignition knob) that starts the engine of the vehicle based on the electronic key being certified by the certifying device of the electronic key for starting the engine and without performing human body certification (figs. 8A and 8B shows the engine start process and that the engine is started without biometrics), the electronic key being an electronic key whose ID information is memorized in the memory, after the vehicle door is unlocked by the door lock control device (fig. 8A shows that at step 12 the method determines if the first ID has been stored from the door unlocking method of figure 7A; ¶0043-0058 discloses this process is all done with one key).

Onuma does not explicitly disclose:

a human body certification information certifying device that confirms human body certification information of the person;

the door lock control device unlocks the door after certifying the key and human body certification;

the memory memorizes data based on certifying the key and human body certification; and

the engine certifying device certifies the key based on detection by an approaching detection sensor and reception of a response signal sent from the key.

However, von Alten discloses receiving two pieces of authentication data to enter the vehicle and only one piece of authentication to start the engine of the vehicle (cols. 1/2, lines 61-67/1-4 discloses to gain access to the vehicle a user has to provide identity information and a user code, and only has to provide a user code for the engine to be started).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to implement in Onuma two pieces of authentication data to gain access to the vehicle and only one to start the engine, as taught by von Alten.

The motivation would be to design a system that requires a higher security to gain access to the vehicle, and a lower security setting to control devices within the vehicle once access is gained into the vehicle.

Onuma and von Alten do not explicitly disclose:

a human body certification information certifying device that confirms human body certification information of the person;

the door lock control device unlocks the door after certifying the key and human body certification;

the memory memorizes data based on certifying the key and human body certification; and

the engine certifying device certifies the key based on detection by an approaching detection sensor and reception of a response signal sent from the key.

Nakamura discloses an anti-theft system for a vehicle, comprising:

a certifying device of an electronic key for getting in the vehicle, the certifying device means being for certifying the electronic key held by a person who intends to get in the vehicle (¶0019);

a human body certification information certifying device confirming that confirms human body certification information of the person (¶0019);

a door lock control device for unlocking a vehicle door (¶0040) in a case where the electronic key is certified by the certifying device of the electronic key for getting in the vehicle (¶0040) and the human body certification information of the person is confirmed by the human body certification information certifying device in a state where the door is locked (¶0087).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify Onuma and von Alten so that the two pieces of authentication data received to unlock a vehicle door are an ID code and biometric data, as taught by Nakamura. The combination of Onuma, von Alten and Nakamura would yield the claim limitation "the memory memorizes data based on certifying the key and human body certification."

The motivation would be to design an access system that would positively prevent a wrongful authentication process (Nakamura ¶0020).

Onuma, von Alten and Nakamura do not explicitly disclose that the engine certifying device certifies the key based on detection by an approaching detection sensor and reception of a response signal sent from the key.

Asakura discloses that an engine start process may be initiated after a vehicle door is unlocked and a door switch (i.e., approaching detection sensor) detects that the vehicle door has been opened and closed. Asakura discloses that after the door switch has detected an opening and closing of a door a demand signal is sent to an electronic key. Once the key has received a demand key the key responds back with a response signal (col. 7, lines 22-33).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to allow Onuma, von Alten and Nakamura engine certifying device to certify the key based on detection by an approaching detection sensor and reception of a response signal sent from the key, as taught by Asakura in order to provide an additional feature to the system that would allow the user to have more hands free for operating other tasks.

3. Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Onuma (Pub. No.: US 2001/0026213 A1) in view of von Alten (Pat. No.: US 6,873,840

B1), Nakarmura (EP 1 286 297 A1), Asakura (Pat. No.: US 6,744,349 B1) and in further view of Sues (Pat. No.: US 5,229,648).

1) In regard to claim 2 (dependent on claim 1), Onuma, von Alten, Nakamura and Asakura disclose the anti-theft system for a vehicle as claimed in claim 1, and that the electronic key is certified by the certifying device of the electronic key for starting the engine and whose ID information is memorized in the memory, after the door is unlocked by the door lock control device (see the rejection of claim 1).

Onuma, von Alten, Nakamura and Asakura do not disclose that the memory memorizes, in advance, a maximum number of times for permitting starting the engine after the door is unlocked by the door lock control device, and the engine starting switch allows for starting of the engine for the permitted maximum number of times memorized in the memory by the electronic key.

Sues discloses that a memory memorizes, in advance, a maximum number of times for permitting starting the engine after the door is unlocked by the door lock control device (col. 3, lines 42-47 discloses the manual override allows a predetermined number of starts) the engine starting switch allows for starting of the engine for the permitted maximum number of times memorized in the memory by the electronic key (col. 3, lines 42-47 discloses the manual override allows a predetermined number of starts).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify Onuma, von Alten, Nakamura and

Asakura vehicle entry and engine start system to have a predetermined number of engine starts, as taught by Sues.

The motivation would be to discourage thieves from stealing the vehicle since it can only be used a certain number of times before needing to reset the number, this would cause the car to have little resale value (Sues col. 4, lines 16-21).

2) In regard to claim 3 (dependent on claim 2), Onuma, von Alten, Nakamura, Asakura and Sues further disclose the anti-theft system for a vehicle as claimed in claim 2, wherein the memory memorizes, in advance, a maximum number of times for permitting starting of the engine after the door is unlocked by the door lock control device (Sues; col. 3, lines 42-47: the manual override allows a predetermined number of starts), the maximum number being set for every electronic key which is certified and registered (Sues; col. 5, lines 61-67: the registered key of the factory, dealer, and customer is set for a predetermined number of starts), and

the engine starting switch allows for starting of the engine for the permitted maximum number of times memorized in the memory by the electronic key which is certified by the certifying device of the electronic key for starting the engine (Sues; col. 3, line 42-47: the manual override allows a predetermined number of starts) and whose ID information is memorized in the memory (Nakamura; Fig. 3a: identification storage section), the maximum number corresponding to the electronic key and being memorized in the memory, after the door is unlocked by the door lock control means

(Sues; col. 3, line 42-47: the manual override allows a predetermined number of starts).

3) In regard to claim 4 (dependent on claim 1), Onuma, von Alten, Nakamura, and Asakura disclose the anti-theft system for a vehicle as claimed in claim 1, that the electronic key is certified by the certifying device of the electronic key for starting the engine and whose ID information is memorized in the memory and the human body certification information is confirmed by the human body information certifying device at the time when the door is unlocked by the door lock control means (see the rejection of claim 1).

Onuma, von Alten, Nakamura, and Asakura do not disclose that the memory memorizes in advance, a maximum number of times for permitting starting of the engine after the door is unlocked by the door lock control device, the maximum number being set for every person who is certified and registered, and the engine starting control device allows for starting of the engine for the permitted maximum number of times memorized in the memory by the electronic key the maximum number corresponding to the person the maximum number being memorized in the memory, after the door is unlocked by the door lock control means.

Sues discloses wherein the memory memorizes in advance, a maximum number of times for permitting starting of the engine after the door is unlocked by the door lock control device (col. 3, lines 42-47: the manual override allows a predetermined number of starts), the maximum number being set for every person who is certified and registered (col. 5, lines 61-67: the registered key of the factory, dealer, and customer is

set for a predetermined number of starts), and the engine starting control device allows for starting of the engine for the permitted maximum number of times memorized in the memory by the electronic key the maximum number corresponding to the person, the maximum number being memorized in the memory, after the door is unlocked by the door lock control means (col. 5, lines 61-67: the registered key of the factory, dealer, and customer is set for a predetermined number of starts).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify Onuma, von Alten, Nakamura, and Asakura vehicle entry and engine start system to have a predetermined number of engine starts, as taught by Sues.

The motivation would be to discourage thieves from stealing the vehicle since it can only be used a certain number of times before needing to reset the number, this would cause the car to have little resale value (Sues col. 4, lines 16-21).

4. Claims 6 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura (EP 1 286 297 A1) in view of Yamasaki (Pat. No.: US 6,075,454) and von Alten (Pat. No.: US 6,873,840 B1).

1) In regard to claim 6, Nakamura discloses an anti-theft system for a vehicle, comprising:

a certifying device of an electronic key for getting in the vehicle (Paragraph 19: portable unit identification), the certifying device the electronic key held by a person who intends to get in the vehicle (Paragraph 19: portable unit identification);

a human body certification information certifying device for confirming human body certification information of the person (Paragraph 19: biometrics information can be used);

a door lock control device for unlocking a vehicle door (Paragraph 40: release the door lock) in a case where the electronic key is certified by the certifying of the electronic key for getting in the vehicle (Paragraph 40: lock system 12 compares the keyless entry IDs) and the human body certification information of the person is confirmed by the human body certification information certifying device in a state where the door is locked (Paragraph 87: the door would have to be locked before it can be unlocked);

a writing device (Paragraph 35: the biometric authenticating section stores the information) that writes information that the human body certification information is confirmed in the electronic key as readable or delete-able information (Paragraph 35: registering and storing biometric information), when the vehicle door is unlocked by the door lock control device based on the electronic key being certified by the certifying device of the electronic key for getting in the vehicle (Paragraph 35 and 36: the biometric reading is confirmed with the biometric database) and the human body certification information of the person being confirmed by the human body certification information certifying device (Paragraph 35 and 36: the biometric reading is confirmed with the biometric database)

a certifying device of an electronic key for starting an engine (Paragraph 87: biometrics authenticates the user), and

an engine starting switch for starting that starts the engine of the vehicle in a case where the electronic key being certified by the certifying device of the electronic key for starting the engine (Paragraph 41: the engine immobilizer controls the engine to on) and the information that the human body certification information is certified is written in the electronic key, after the vehicle door is unlocked by the door lock control device (Paragraph 35 and 36: the biometric reading is confirmed with the biometric database).

Nakamura does not disclose the engine certifying device for certifying the electronic key is based on a detection by an approaching detection sensor and reception a response signal sent from the electronic key held by a person who intends to start the engine.

Yamasaki discloses a certifying device means for certifying the electronic key based on a detection by an approaching detection sensor (col. 2 lines 46-48: proximity sensor detects the approach of the remote control) and reception a response signal sent from the electronic key held by a person who intends to start the engine (Fig. 5: remote control sends a response signal s33).

At the time of invention, it would have been obvious to a person with ordinary skill in the art to modify Nakamura's vehicle entry and engine start system to certify a key based on the approach, as taught by Yamasaki.

The motivation would be to allow the user to have more hands free for operating other tasks (col. 1 lines 53-56).

Nakamura and Yamasaki do not explicitly disclose that the second operation is permitted without performing human body certification after the first operation is performed.

However, von Alten discloses receiving two pieces of authentication data to enter the vehicle and only one piece of authentication to start the engine of the vehicle (cols. 1/2, lines 61-67/1-4 discloses to gain access to the vehicle a user has to provide identity information and a user code, and only has to provide a user code for the engine to be started).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement in Nakamura and Yamasaki a process that requires two pieces of information for a first operation and only one piece of information for a second operation, since it has been held that omission of an element and its function in a combination where the remaining elements perform the same functions as before involves only routine skill in the art. In re Karlson, 136 USPQ 184.

2) In regard to claim 12, Nakamura discloses an anti-theft system for a vehicle, comprising:

a certifying device of an electronic key for starting a vehicle engine (Paragraph 19: portable unit identification), the certifying device certifying the electronic key held by a person who intends to start the vehicle (Paragraph 19: portable unit identification);

a human body certification information certifying device that confirms human body certification information of the person (Paragraph 19: biometrics information can be used);

an engine starting control switch that starts the engine in a case where the electronic key is certified by the certifying device of the electronic key for starting the engine (Paragraph 41: the engine immobilizer controls the engine to on) and the human body certification information of the person is confirmed by the human body certification information certifying device (Paragraph 35 and 36: the biometric reading is confirmed with the biometric database) in a state where the engine has stopped running (Paragraph 41: the immobilizer starts the engine based on the certification of the user, therefore the engine would not be running when it is verifying the user);

a writing device for writing information that the human body certification information is confirmed to the electronic key as readable or delete-able information (Paragraph 35 and 36: the biometric reading is confirmed with the biometric database), when the engine is started by the engine starting switch based on the electronic key being certified by the certifying device of the electronic key for starting the engine (Paragraph 41: the immobilizer controls the engine by comparing the ID information) and the human body certification information of the person being confirmed by the human body certification information certifying device (Paragraph 87: the biometrics authentication is verified);

a certifying device of an electronic key for starting an engine (Paragraph 19: portable unit identification), and

a door locking control device that unlocks the door based on the electronic key being certified by the certifying device of the electronic key for getting in the vehicle (Paragraph 40: release the door lock), and information that the human body certification information is confirmed is written in the electronic key, after the engine is started by the engine starting control device (Paragraph 35 and 36: the biometric reading is confirmed with the biometric database).

Nakamura does not disclose the certifying device certifies the electronic key based on a detection by an approaching detection sensor and reception of a response signal sent from the electronic key held by a person who intends to start the engine.

Yamasaki discloses a certifying device may certify an electronic key based on a detection by an approaching detection sensor (col. 2 lines 46-48: proximity sensor detects the approach of the remote control) and reception of a response signal sent from the electronic key held by a person who intends to start the engine (Fig. 5: remote control sends a response signal s33), the response signal sent in response to an initial request signal sent by the approaching detection sensor (Fig. 5: onboard module transmits an interrogation signal s31).

At the time of invention, it would have been obvious to a person with ordinary skill in the art to modify Nakamura's vehicle entry and engine start system to certify a key based on the approach, as taught by Yamasaki.

The motivation would be to allow the user to have more hands free for operating other tasks (col. 1, lines 53-56).

Nakamura and Yamasaki do not explicitly disclose that the second operation is permitted without performing human body certification after the first operation is performed.

However, von Alten discloses receiving two pieces of authentication data to enter the vehicle and only one piece of authentication to start the engine of the vehicle (cols. 1/2, lines 61-67/1-4 discloses to gain access to the vehicle a user has to provide identity information and a user code, and only has to provide a user code for the engine to be started).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement in Nakamura and Yamasaki a process that requires two pieces of information for a first operation and only one piece of information for a second operation, since it has been held that omission of an element and its function in a combination where the remaining elements perform the same functions as before involves only routine skill in the art. In re Karlson, 136 USPQ 184.

5. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura (EP 1 286 297) in view of Funakoshi (Pat. No.: US 5,861,816), Yamasaki (Pat. No.: US 6,075,454) and von Alten (Pat. No.: US 6,873,840 B1).

1) In regard to claim 7, Nakamura discloses an anti-theft system for a vehicle, comprising:

a certifying device of an electronic key for starting a vehicle engine (Paragraph 19: portable unit identification), the certifying device certifying the electronic key held by a person who intends to start the vehicle (Paragraph 19: portable unit identification);

a human body certification information certifying device for confirming human body certification information of the person (Paragraph 19: biometrics information can be used);

an engine starting switch that starts the engine in a case where the electronic key is certified by the certifying device of the electronic key for starting the engine (Paragraph 41: the engine immobilizer controls the engine to on) and the human body certification information of the person is confirmed by the human body certification information certifying device in a state where the engine is-has stopped running (Paragraph 41: the immobilizer starts the engine based on the certification of the user, therefore the engine would not be running when it is verifying the user); and

the human body certification information of the person being confirmed by the human body certification information certifying device (Paragraph 87: the biometrics authentication is verified);

a certifying device of an electronic key for starting an engine a door locking control device means that unlocks the door in a case where the electronic key is certified (Paragraph 40: release the door lock) by the certifying device of the electronic key for getting in the vehicle (Paragraph 40: keyless entry system).

Nakamura does not disclose a memory that memorizes ID information of the electronic key when the engine is started by the engine starting control device based on

the electronic key being certified by the certifying device of the electronic key for starting the engine and the certifying device certifying the electronic key based on a detection by an approaching detection sensor and reception of a response signal sent from the electronic key held by a person who intends to start the engine, and the electronic key is an electronic key whose ID information is memorized in the memory, after the engine is started by the engine starting control device.

Funakoshi discloses a memory that memorizes ID information of the electronic key when the engine is started by the engine starting control device (col. 5 lines 19-22: the updated code is stored at the next engine startup) based on the electronic key being certified by the certifying device of the electronic key for starting the engine (col. 1 lines 60-63: the electronic code corresponds with the built in code) and the electronic key is an electronic key whose ID information is memorized in the memory, after the engine is started by the engine starting control device (col. 5 lines 19-22: the updated code is stored at the next engine startup).

At the time of invention, it would have been obvious to a person with ordinary skill in the art to modify Nakamura's vehicle entry and engine start system to memorize the key ID after the engine start, as taught by Funakoshi.

The motivation would be to utilize known techniques in the art for obtaining key ID for a vehicle security system.

The Supreme Court in KSR International Co. v. Teleflex Inc., identified a number of rationales to support a conclusion of obviousness which are consistent with the proper "functional approach" to the determination of obviousness as laid down in

Graham. The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit.

See MPEP Section 2143.

Nakamura in view of Funakoshi does not disclose the certifying device certifying the electronic key based on a detection by an approaching detection sensor and reception of a response signal sent from the electronic key held by a person who intends to start the engine.

Yamasaki discloses the certifying device certifying the electronic key based on a detection by an approaching detection sensor (col. 2 lines 46-48: proximity sensor detects the approach of the remote control) and reception of a response signal sent from the electronic key held by a person who intends to start the engine (Fig. 5: remote control sends a response signal s33).

At the time of invention, it would have been obvious to a person with ordinary skill in the art to modify Nakamura in view of Funakoshi's vehicle entry and engine start system to certify a key based on the approach, as taught by Yamasaki.

The motivation would be to allow the user to have more hands free for operating other tasks (col. 1 lines 53-56).

Nakamura, Funakoshi, and Yamasaki do not explicitly disclose that the second operation is permitted without performing human body certification after the first operation is performed.

However, von Alten discloses receiving two pieces of authentication data to enter the vehicle and only one piece of authentication to start the engine of the vehicle (cols. 1/2, lines 61-67/1-4 discloses to gain access to the vehicle a user has to provide identity information and a user code, and only has to provide a user code for the engine to be started).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement in Nakamura and Yamasaki a process that requires two pieces of information for a first operation and only one piece of information for a second operation, since it has been held that omission of an element and its function in a combination where the remaining elements perform the same functions as before involves only routine skill in the art. In re Karlson, 136 USPQ 184.

6. Claims 8-9 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura (EP 1 286 297) in view of Funakoshi (Pat. No.: US 5,861,816), Yamasaki (Pat. No.: US 6,075,454), von Alten (Pat. No.: US 6,873,840 B1) and further in view of Denison (PG-Pub 2002/0097141).

1) In regard to claim 8 (dependent on claim 7), Nakamura, Funakoshi, Yamasaki and von Alten disclose the electronic key is certified by the certifying device of the electronic key for getting in the vehicle (Nakamura; Paragraph 40: keyless entry system)

and whose ID information is memorized in the memory after the engine is started by the engine starting control device (Funakoshi; col. 5 lines 19-22: the updated code is stored at the next engine startup) and unlocking the door after the engine is started by the engine starting (Nakamura; Paragraph 116: the user is able to unlock the engine and door).

Nakamura, Funakoshi, Yamasaki and von Alten do not disclose wherein the memory memorizes, in advance, a maximum number of times for permitting unlocking the door and the door locking control device allows for unlocking of the door for the permitted maximum number of times memorized in the memory by the electronic key.

Denison discloses wherein the memory memorizes, in advance, a maximum number of times for permitting unlocking the door (Paragraph 105: the number of allowed accesses decrements after each access) and the door locking control device allows for unlocking of the door for the permitted maximum number of times memorized in the memory by the electronic key (Paragraph 105: the number of allowed accesses decrements after each access).

At the time of invention, it would have been obvious to a person with ordinary skill in the art to modify Nakamura, Funakoshi, Yamasaki and von Alten vehicle entry and engine start system to allow only a certain number of accesses, as taught by Denison.

The motivation would be to prevent unauthorized usage of keys (Paragraph 106).

2) In regard to claim 9 (dependent on claim 7), Nakamura, Funakoshi, Yamasaki and von Alten disclose the electronic key is certified by the certifying device of the

electronic key for getting in the vehicle (Nakamura; Paragraph 40: keyless entry system) and whose ID information is memorized in the memory (Nakamura; Fig. 3a: storage section 14) and the door is unlocked after the engine is started by the engine starting switch (Nakamura; Paragraph 116: the user is able to unlock the engine and door).

Nakamura, Funakoshi, Yamasaki and von Alten do not disclose wherein the memory memorizes, in advance, a maximum number of times for permitting unlocking of the door the maximum number of times being set for every electronic key which is certified and registered, and the door locking control device that allows for unlocking of the door for the permitted maximum number of times memorized in the memory by the electronic key.

Denison discloses wherein the memory memorizes, in advance, a maximum number of times for permitting unlocking of the door the maximum number of times being set for every electronic key which is certified and registered (Paragraph 105: the number of allowed accesses decrements after each access), and the door locking control device that allows for unlocking of the door for the permitted maximum number of times memorized in the memory by the electronic key (Paragraph 105: the number of allowed accesses decrements after each access).

At the time of invention, it would have been obvious to a person with ordinary skill in the art to modify Nakamura, Funakoshi, Yamasaki and von Alten vehicle entry and engine start system to allow only a certain number of accesses, as taught by Denison.

The motivation would be to prevent unauthorized usage of keys (Paragraph 106).

3) In regard to claim 10 (dependent on claim 7), Nakamura, Funakoshi, Yamasaki, von Alten and Denison disclose wherein the door locking control device includes a permission counter number (Denison; Paragraph 105: the number of allowed accesses decrements after each access) that reduces the number of times permission is granted to unlock for unlocking the door by using the electronic key (Denison; Paragraph 105: the number of allowed accesses decrements after each access) that is certified by the certifying device of the electronic key for getting in the vehicle and whose ID information is memorized in the memory (Nakamura; Paragraph 40: the keyless entry), when the vehicle door is unlocked and then opened (Denison; Paragraph 105: the counter decrements only after each access, which would mean the user would have to unlock and open the door before the user would have access).

7. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura (EP 1 286 297) in view of Funakoshi (Pat. No.: US 5,861,816), Yamasaki (Pat. No.: US 6,075,454), von Alten (Pat. No.: US 6,873,840 B1) and further in view of Denison (PG-Pub No.: US 2002/0097141) and Goodman et al. (PG-Pub No.: US 2002/0043566).

1) In regard to claim 10 (dependent on claim 7), Nakamura, Funakoshi, Yamasaki and von Alten disclose that the electronic key is certified by the certifying device of the electronic key for getting in the vehicle (Nakamura; Paragraph 40: keyless entry system) and whose ID information is memorized in the memory (Funakoshi; col. 5 lines 19-22: the updated code is stored at the next engine startup), and unlocking the

door after the engine is started by the engine starting switch (Nakamura; Paragraph 116: the user is able to unlock the engine and door) the human body certification is confirmed at the time when the engine is started by the engine starting switch (Paragraph 87: the biometric authenticating section determines a match, Paragraph 126 the processes can be executed in any order).

Nakamura, Funakoshi, Yamasaki and von Alten do not disclose wherein the memory memorizes, in advance, a maximum number of times for permitting unlocking of the door the maximum number being set for every person who is certified and registered, and the door locking control device allows for unlocking of the door for the permitted maximum number of times memorized in the memory by the electronic key the maximum number being memorized in the memory the maximum number corresponding to the person whose human body certification information is confirmed by the human body information certifying device.

Denison discloses wherein the memory memorizes, in advance, a maximum number of times for permitting unlocking of the door (Paragraph 105: the number of allowed accesses decrements after each access) the maximum number being set for every person who is certified and registered (Paragraph 105: each master key), and the door locking control device allows for unlocking of the door for the permitted maximum number of times memorized in the memory by the electronic key the maximum number being memorized in the memory (Paragraph 105: the number of allowed accesses decrements after each access).

At the time of invention, it would have been obvious to a person with ordinary skill

in the art to modify Nakamura, Funakoshi, Yamasaki and von Alten vehicle entry and engine start system to allow only a certain number of accesses, as taught by Denison.

The motivation would be to prevent unauthorized usage of keys (Paragraph 106).

Nakamura, Funakoshi, Yamasaki, von Alten and Denison do not disclose the maximum number corresponding to the person whose human body certification information is confirmed by the human body information certifying device.

Goodman discloses the maximum number corresponding to the person whose human body certification information is confirmed by the human body information certifying device (Paragraph 22: biometric sensors are used, Paragraph 38: the count decrements every time it is activated).

At the time of invention, it would have been obvious to a person with ordinary skill in the art to modify Nakamura, Funakoshi, Yamasaki, von Alten and Denison vehicle entry and engine start system to allow only a certain number of accesses, as taught by Goodman.

The motivation would be to prevent the use of counterfeits (Paragraph 6, Paragraph 11).

Allowable Subject Matter

8. Claim 5 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

9. Applicant's arguments with respect to claims 1-12 have been considered but are moot in view of the new ground(s) of rejection necessitated by the amendments to the claims.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1) Nagai (Pub. No.: US 2004/0085189 A1)

-- discloses a detection zone for the exterior of a vehicle and interior of the vehicle

2) Perttunen (Pat. No.: US 6,891,467 B2)

-- discloses the vehicle stores the FOB ID when received

3) Tumey (Pub. No.: US 2002/0097145 A1)

-- discloses receiving facial images to allow entry into a vehicle

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Curtis J. King whose telephone number is (571)270-5160. The examiner can normally be reached on Mon-Thurs 7:30 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Benjamin C. Lee can be reached on (571)272-2963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ck/

/BENJAMIN C. LEE/

Supervisory Patent Examiner, Art Unit 2612